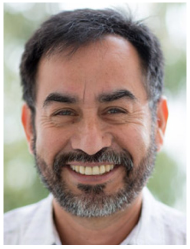
The Set of Zero Divisors of a Factor Ring

Jesús Jiménez (Point Loma Nazarene University)



Jesús Jiménez earned his Ph.D. in Mathematics from the University of Utah, and the M.S. and B.S. from the National Autonomous University of Mexico. His specializations are algebraic geometry and cryptology. He spends time each summer teaching coding theory and cryptography at the Center for Research in Mathematics at the University of Guanajuato in Guanajuato, Mexico, as well as teaching origami to Chiapas high schoolers using the theorems of geometry. He enjoys cooking and volleyball.

Abstract

We show that if A is a commutative ring with unity and $\mathfrak{a}$ is an ideal of A which is a finite product of relative prime ideals $\mathfrak{b}_i$ then the factor ring $A/\mathfrak{a}$ is a direct sum of ideals $\mathfrak{a}_i/\mathfrak{a}$. Moreover, each ideal $\mathfrak{a}_i/\mathfrak{a}$ endowed with addition and multiplication modulo $\mathfrak{a}$ is a ring isomorphic to the factor ring $A/\mathfrak{b}_i$. We give examples when A is the ring of integers $\mathbb{Z}$, the Gaussian integers $\mathbb{Z}[\mathbf{i}]$, or a ring of polynomials $\mathbb{F}_q[x]$ over a finite field with q elements $\mathbb{F}_q$.

1 Introduction

Throughout this paper A will be a commutative ring with a non-zero multiplicative identity. The group of units of A will be denoted by $U(A)$ and the set of zero divisors together with the zero element will be denoted by $Z(A)$. If A is finite then the set $Z(A)$ is the complement of $U(A)$, Lemma 1. In [2] and [6], the authors show that if $A = \mathbb{Z}_a$, the ring of integers modulo a, then there exist positive integers n such that $U(\mathbb{Z}_a)$ can be mapped isomorphically to a group D contained in the set $Z(\mathbb{Z}_n)$ with the group structure of D given by multiplication modulo n. Here we will show, by means of the Chinese Remainder Theorem, that there exist positive integers n such that the ring $\mathbb{Z}_a$ can be mapped, ring isomorphically, to a ring R contained in the set $Z(\mathbb{Z}_n)$ with the ring structure of R given by addition and multiplication modulo n. This shows that the group $U(\mathbb{Z}_a)$ is isomorphic to $U(R) \subset R \subset Z(\mathbb{Z}_n)$.

2 Elements of Ring Theory

An element x of a A is *nilpotent* if and only if there exists a positive integer n such that $x^n = 0$. An element e of a A is *idempotent* if and only if $e^2 = e$. If e_1 and e_2 are nonzero idempotent elements of A, we say that they are *orthogonal* if and only if $e_1 \cdot e_2 = 0$. We remark that if an element y of A is both nilpotent and idempotent then $y = 0$. We say that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A are *relatively prime* or *coprime* if and only if $\mathfrak{a} + \mathfrak{b} = A$. A proper ideal $\mathfrak{m}$ of A is a *maximal* ideal if and only if for any ideal $\mathfrak{a}$ of A such that $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ either $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{a} = A$. A ring A is called a *local ring* if and only if it has only one proper maximal ideal $\mathfrak{m}$. If $A_1, A_2, \ldots, A_k$ are rings then the *direct product* of these rings is the ring

$$A_1 \times A_2 \times \cdots A_k$$

with component-wise addition and multiplication.

Lemma 1. *If A is a finite ring then $Z(A) = A \setminus U(A)$.*

Proof. First, we observe that $U(A) \cap Z(A) = \emptyset$ since a unit may not be a zero divisor. Next, let $a \neq 0$ be an element of A and define the homomorphism $\mu_a : A \to A$ (A consider as a commutative group under addition) by $\mu_a(x) = ax$. If μ_a is not injective then μ_a has a nonzero kernel so there exists $b \neq 0$ in A such that $\mu_a(b) = ab = 0$ and it follows that a is a zero divisor.
Otherwise, since A is finite, if μ_a is injective μ_a must be onto. Therefore, there exists $c \neq 0$ in A such that $\mu_a(c) = ac = 1$. This implies that a is a unit. $\square$

Lemma 2. *If A is a local ring then the only idempotent elements of A are either* 0 *or* 1.

Proof. Let $\mathfrak{m}$ be the maximal ideal of A and e an idempotent of A. We observe that in a local ring an element x is either in $\mathfrak{m}$ or is a unit. Also, it is not possible to have both e and $1 - e$ be elements of $\mathfrak{m}$ since this implies that $1 = e + (1 - e)$ is in $\mathfrak{m}$ which contradicts the fact that $\mathfrak{m}$ is a proper ideal. Therefore, either e is a unit or $1 - e$ is a unit. Since $e = e^2$, we have $e \cdot (1 - e) = 0$. If e is a unit then $1 - e = 0$, this implies that $e = 1$. On the other hand, if $1 - e$ is a unit then $e = 0$. $\square$

Lemma 3. *Let $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_k$, be ideals of a ring A. Assume that $\mathfrak{b}_i + \mathfrak{b}_j = A$ whenever $i \neq j$. Let $\mathfrak{a}_i = \prod_{j \neq i} \mathfrak{b}_j$. Then, for all $i = 1, 2, \ldots, k$, $\mathfrak{b}_i + \mathfrak{a}_i = A$.*

Proof. For every $j \neq i$ let $a_j \in \mathfrak{b}_j$ and $b_i \in \mathfrak{b}_i$ be such that $a_j + b_i = 1$. Then,

$$a_i = \prod_{j \neq i} a_j = \prod_{j \neq i} (1 - b_i) \equiv 1 \bmod \mathfrak{b}_i.$$

This implies that $a_i - 1 \in \mathfrak{b}_i$. So, there exists $b_i \in \mathfrak{b}_i$ such that $a_i + b_i = 1$. This shows that $\mathfrak{a}_i + \mathfrak{b}_i = A$. $\square$

Lemma 4. *Let $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_k$ be ideals of ring A. Assume that $\mathfrak{b}_i + \mathfrak{b}_j = A$ whenever $i \neq j$. Then,*

$$\prod_{i=1}^{k} \mathfrak{b}_i = \bigcap_{i=1}^{k} \mathfrak{b}_i.$$

Proof. We will use induction on k. If $k = 2$ then $\mathfrak{b}_1$ is relatively prime to $\mathfrak{b}_2$ by assumption. Let $b_1 \in \mathfrak{b}_1$ and $b_2 \in \mathfrak{b}_2$ be such that $b_1 + b_2 = 1$. If $x \in \mathfrak{b}_1 \cap \mathfrak{b}_2$ then $x = xb_1 + xb_2 \in \mathfrak{b}_1\mathfrak{b}_2$. Since $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{b}_1 \cap \mathfrak{b}_2$, it follows that $\mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{b}_1 \cap \mathfrak{b}_2$. Assume that $k \geq 3$. By Lemma 3, $\mathfrak{b}_1$ is relatively prime to $\prod_{i \geq 2} \mathfrak{b}_i$. By the case $k = 2$

$$\mathfrak{b}_1 \cdot \prod_{i \geq 2}^{k} \mathfrak{b}_i = \mathfrak{b}_1 \bigcap \prod_{i \geq 2}^{k} \mathfrak{b}_i.$$

By induction hypothesis

$$\prod_{i \geq 2}^{k} \mathfrak{b}_i = \bigcap_{i \geq 2}^{k} \mathfrak{b}_i.$$

The last two equations show that

$$\prod_{i=1}^{k} \mathfrak{b}_i = \bigcap_{i=1}^{k} \mathfrak{b}_i.$$

This completes the proof. $\square$

Lemma 5. *Let $\mathfrak{a}$ and $\mathfrak{b}$ ideals of A such that $\mathfrak{a}+\mathfrak{b}=A$. Let $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ be such that $a+b=1$. Let $A/\mathfrak{a}$, $A/\mathfrak{b}$, $A/\mathfrak{ab}$ be the factor rings of A by the ideals $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{ab}$ respectively. Then, the ring morphism*

$$\pi : A/\mathfrak{ab} \to A/\mathfrak{a} \times A/\mathfrak{b},\ (x \bmod \mathfrak{ab}) \mapsto (x \bmod \mathfrak{a}, x \bmod \mathfrak{b})$$

is an isomorphism and the ideals $\mathfrak{a}/\mathfrak{ab}$ and $\mathfrak{b}/\mathfrak{ab}$ endowed with addition and multiplication modulo $\mathfrak{ab}$ are rings with unity. Moreover, the unity of $\mathfrak{a}/\mathfrak{ab}$ is $a \bmod \mathfrak{ab}$, the unity of $\mathfrak{b}/\mathfrak{ab}$ is $b \bmod \mathfrak{ab}$ and the ring morphisms

$$\begin{aligned}
&\mathfrak{a}/\mathfrak{ab} \to A/\mathfrak{b},\ (x \bmod \mathfrak{ab}) \mapsto (x \bmod \mathfrak{b}) \quad \textit{and} \\
&\mathfrak{b}/\mathfrak{ab} \to A/\mathfrak{a},\ (y \bmod \mathfrak{ab}) \mapsto (y \bmod \mathfrak{a})
\end{aligned}$$

are isomorphisms.

Proof. The ring morphism

$$A \to A/\mathfrak{a} \times A/\mathfrak{b},\ (x \mapsto (x \bmod \mathfrak{a}, x \bmod \mathfrak{b})$$

is well defined and surjective and its kernel is $\mathfrak{a} \cap \mathfrak{b}$. By Lemma 3, $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. This implies that π is an isomorphism. Since $a+b=1$ we have

$$(b \bmod \mathfrak{ab}) \mapsto (b \bmod \mathfrak{a}) = (1 - a \bmod \mathfrak{a}) = (1 \bmod \mathfrak{a}).$$

Now we show that $\mathfrak{b}/\mathfrak{ab} \to A/\mathfrak{a}$ is surjective. Let $(x \bmod \mathfrak{a}) \in A/\mathfrak{a}$. We have $bx \in \mathfrak{b}$ and

$$\begin{aligned}
(bx \bmod \mathfrak{ab}) \mapsto (bx \bmod \mathfrak{a}) &= (b \bmod \mathfrak{a})(x \bmod \mathfrak{a}) \\
&= (1 \bmod \mathfrak{a})(x \bmod \mathfrak{a}) \\
&= (x \bmod \mathfrak{a}).
\end{aligned}$$

Next we show that $\mathfrak{b}/\mathfrak{ab} \to A/\mathfrak{a}$ is injective. If y_1 and y_2 are in $\mathfrak{b}$ and

$$(y_1 \bmod \mathfrak{a}) = (y_2 \bmod \mathfrak{a})$$

then $y_1 - y_2 \in \mathfrak{a}$. It follows that $y_1 - y_2 \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$. This implies that

$$(y_1 \bmod \mathfrak{ab}) = (y_2 \bmod \mathfrak{ab}).$$

and it follows that the morphism is injective. Therefore, the morphism is an isomorphism. $\square$

Theorem 6 (Chinese Remainder Theorem)**.** *Let $\mathfrak{b}_1, \mathfrak{b}_2, \ldots \mathfrak{b}_k$, be ideals in A. Set $\mathfrak{a} = \prod \mathfrak{b}_i$ and assume that $\mathfrak{b}_i + \mathfrak{b}_j = A$ whenever $i \neq j$. Then, the ring morphism*

$$\pi : A/\mathfrak{a} \to A/\mathfrak{b}_1 \times A/\mathfrak{b}_2 \times \cdots \times A/\mathfrak{b}_k,\ \pi(x \bmod \mathfrak{a}) = (x \bmod \mathfrak{b}_1, x \bmod \mathfrak{b}_2, \ldots, x \bmod \mathfrak{b}_k)$$

is a ring isomorphism.

Proof. We will use induction on k. If $k = 1$ there is nothing to prove. Assume that $k = 2$. Since $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are relatively prime the result follows from Lemma 5. Suppose that $k \geq 3$. By Lemma 3, $\mathfrak{b}_1$ is relatively prime to the product $\prod_{i\geq 2}^{k} \mathfrak{b}_i$. Therefore,

$$\begin{aligned} A/\mathfrak{a} &= A/(\mathfrak{b}_1 \cdot (\mathfrak{b}_2 \cdots \mathfrak{b}_k)) \\ &\simeq A/\mathfrak{b}_1 \times A/(\mathfrak{b}_2 \cdots \mathfrak{b}_k), \text{ (by Lemma 5)} \\ &\simeq A/\mathfrak{b}_1 \times A/\mathfrak{b}_2 \times \mathfrak{b}_3 \times \cdots \times A/\mathfrak{b}_k \text{ (by induction hypothesis).} \end{aligned}$$

□

Corollary 7. *Let*

$$\pi : A/\mathfrak{a} \to A/\mathfrak{b}_1 \times A/\mathfrak{b}_2 \times \cdots \times A/\mathfrak{b}_k,\ \pi(x \bmod \mathfrak{a}) = (x \bmod \mathfrak{b}_1, x \bmod \mathfrak{b}_2, \ldots, x \bmod \mathfrak{b}_k)$$

be as in Theorem 6, $\pi_i : A/\mathfrak{b}_1 \times A/\mathfrak{b}_2 \times \cdots \times A/\mathfrak{b}_k \to A/\mathfrak{b}_i$ be the canonical projection, and $\mathfrak{a}_i = \prod_{j\neq i} \mathfrak{b}_j$. Then $\mathfrak{a}_i/\mathfrak{a}$ endowed with addition and multiplication modulo $\mathfrak{a}$ is a ring with unity and

$$\pi_i \circ \pi\ |_{\mathfrak{a}_i/\mathfrak{a}} \colon \mathfrak{a}_i/\mathfrak{a} \to A/\mathfrak{b}_i$$

is an isomorphism.

Proof. This follows from Lemma 5 since $\mathfrak{a}_i$ is relatively prime to $\mathfrak{b}_i$ and $\mathfrak{a} = \mathfrak{a}_i\mathfrak{b}_i$. □

Corollary 8. *Let $\mathfrak{a}_i$ be as in Corollary 7 and $e_i \in \mathfrak{a}_i$ be such that $e_i \equiv 1 \bmod \mathfrak{b}_i$. Then e_i is an idempotent in $\mathfrak{a}_i$ for all $i = 1, 2, \ldots, k$, e_i is orthogonal to e_j whenever $i \neq j$, and $e = e_1 + e_2 + \cdots + e_k \equiv 1 \bmod \mathfrak{a}$. Moreover, e_i is the multiplicative identity of $\mathfrak{a}_i/\mathfrak{a}$*

Proof. Since the map $\pi_i \circ \pi\ |_{\mathfrak{a}_i/\mathfrak{a}}$ is an isomorphism and

$$\pi_i \circ \pi\ |_{\mathfrak{a}_i/\mathfrak{a}} (e_i^2 \bmod \mathfrak{a}) \equiv 1 \bmod \mathfrak{a} \equiv \pi_i \circ \pi\ |_{\mathfrak{a}_i/\mathfrak{a}} (e_i \bmod \mathfrak{a})$$

we have $e_i^2 \equiv e_i \bmod \mathfrak{a}$ for all $i = 1, 2, \ldots, k$. Now, if $i \neq j$ then $e_i \cdot e_j \in \mathfrak{a}_i\mathfrak{a}_j \subseteq \mathfrak{a}$ and it follows that $e_i \cdot e_j \equiv 0 \bmod \mathfrak{a}$. Also, since

$$\pi(e \bmod \mathfrak{a}) = (1 \bmod \mathfrak{b}_1, 1 \bmod \mathfrak{b}_2, \ldots, 1 \bmod \mathfrak{b}_k) = \pi(1 \bmod \mathfrak{a})$$

we have $e \equiv 1 \bmod \mathfrak{a}$. That e_i is the multiplicative identity of $\mathfrak{a}_i/\mathfrak{a}$ follows from Lemma 5. □

Corollary 9. *Let $\mathfrak{a}_i$ and $e_i \in \mathfrak{a}_i$ be such that $e_i \equiv 1 \bmod \mathfrak{b}_i$, then $A/\mathfrak{a} = \mathfrak{a}_1 + \mathfrak{a}_2 + \cdots + \mathfrak{a}_k$ and every element $x \in A$ can be uniquely written as $xe_1 + xe_2 + \cdots + xe_k \equiv x \bmod \mathfrak{a}$. That is, A is the direct sum of the ideals $\mathfrak{a}_i$.*

Proof. Since $e_1 + e_2 + \cdots + e_k \equiv 1 \bmod \mathfrak{a}$ it follows that $xe_1 + xe_2 + \cdots + xe_k \equiv x \bmod \mathfrak{a}$. To show that this representation is unique it suffices to show that if $xe_1 + xe_2 + \cdots + xe_k \equiv 0 \bmod \mathfrak{a}$ then $x \equiv 0 \bmod \mathfrak{a}$. Since

$$0 \bmod \mathfrak{a} = \pi_i \circ \pi\ |_{\mathfrak{b}_i/\mathfrak{a}} (0) = \pi_i \circ \pi\ |_{\mathfrak{b}_i/\mathfrak{a}} (xe_1 + xe_2 + \cdots + xe_k) = xe_i \bmod \mathfrak{a}_i = x \bmod \mathfrak{a}_i$$

it follows that $x \in \mathfrak{a}_i$ for all $i = 1, 2, \ldots, k$ so $x \in \cap_{i=1}^{k} \mathfrak{a}_i = \mathfrak{a}$. This shows that $x \equiv 0 \bmod \mathfrak{a}$. □

3 Factor rings of the ring of integers

Let $\mathbb{Z}_a$ be the ring of integers modulo a. The set $U(\mathbb{Z}_a)$ consists of all the elements in $\mathbb{Z}_n$ which are relatively prime to n. The number of elements of $U(\mathbb{Z}_a)$ is $\varphi(a)$, where $\varphi(a)$ is the Euler function. $U(\mathbb{Z}_a)$ is a group under multiplication modulo a and its group structure is well known. Recall that the set $Z(\mathbb{Z}_a)$ is the complement of $U(\mathbb{Z}_a)$ in $\mathbb{Z}_a$. The nonzero elements of $Z(\mathbb{Z}_a)$ are zero divisors under multiplication modulo a. The set $Z(\mathbb{Z}_a)$ is closed under multiplication modulo a, since the product of zero divisors is a zero or a zero divisor. At first sight, it seems that there is no hope of finding subsets of $Z(\mathbb{Z}_a)$ that could be groups under multiplication modulo a. However, as we will show in the example below, there are subsets of $Z(\mathbb{Z}_a)$ that are not only ideals of $\mathbb{Z}_a$ but are rings with unity when endowed with addition and multiplication modulo a and the units of these rings are groups under multiplication modulo a. See [2], [6]. The example below illustrates the central theme of this paper.

Example 10. *Consider the ring $\mathbb{Z}_{360}$. The sets*

$$\begin{aligned} Z_5 &= \{0, 72, 144, 216, 288\} = 72\mathbb{Z}_{360}, \\ Z_8 &= \{0, 45, 90, 135, 180, 225, 270, 315\} = 45\mathbb{Z}_{360}, \text{ and} \\ Z_9 &= \{0, 40, 80, 120, 160, 200, 240, 280, 320\} = 40\mathbb{Z}_{360} \end{aligned}$$

are principal ideals of $\mathbb{Z}_{360}$. These ideals are rings with unity under addition and multiplication modulo 360. The multiplicative identities of the ideals Z_5, Z_8 and Z_9 are $e_5 = 216 \bmod 360$, $e_8 = 225 \bmod 360$, and $e_9 = 280 \bmod 360$ respectively. The element 0 is the additive identity for them. The ring isomorphisms and their inverses are given below.

$$\begin{array}{lcllcl} \theta_{216} : Z_5 & \to & \mathbb{Z}_5 & \theta_{216}(72x \bmod 360) & = & 72x \bmod 5 \\ \theta_{225} : Z_8 & \to & \mathbb{Z}_8 & \theta_{225}(45x \bmod 360) & = & 45x \bmod 8 \\ \theta_{280} : Z_9 & \to & \mathbb{Z}_9 & \theta_{280}(40x \bmod 360) & = & 40x \bmod 9 \end{array}$$

$$\begin{array}{lcllcl} \theta_{216}^{-1} : \mathbb{Z}_5 & \to & Z_5 & \theta_{216}^{-1}(x \bmod 5) & = & 216x \bmod 360 \\ \theta_{225}^{-1} : \mathbb{Z}_8 & \to & Z_8 & \theta_{225}^{-1}(x \bmod 8) & = & 225x \bmod 360 \\ \theta_{280}^{-1} : \mathbb{Z}_9 & \to & Z_9 & \theta_{280}^{-1}(x \bmod 9) & = & 280x \bmod 360 \end{array}$$

The elements, e_5, e_8, and e_9 satisfy

$$e_5 \cdot e_8 \equiv e_5 \cdot e_9 \equiv e_8 \cdot e_9 \equiv 0 \bmod 360$$

and

$$e_5 + e_8 + e_9 \equiv 1 \bmod 360.$$

Therefore, for all $x \in \mathbb{Z}_{360}$, we have

$$xe_5 + xe_8 + xe_9 \equiv x \bmod 360$$

and this representation is unique. That is,

$$\mathbb{Z}_{360} = e_5\mathbb{Z}_{360} \oplus e_8\mathbb{Z}_{360} \oplus e_9\mathbb{Z}_{360}.$$

The other nonzero proper ideals of $\mathbb{Z}_{360}$ (besides Z_5, Z_8, Z_9) that are rings with addition and multiplication modulo 360 are

Ideal	*Identity*				
$Z_5 \oplus Z_8$	$e_5 + e_8$	$\equiv$	$216 + 225$	$\equiv$	$81 \bmod 360$
$Z_5 \oplus Z_9$	$e_5 + e_9$	$\equiv$	$216 + 280$	$\equiv$	$136 \bmod 360$
$Z_8 \oplus Z_9$	$e_8 + e_9$	$\equiv$	$225 + 280$	$\equiv$	$145 \bmod 360$

We have the following general result.

Corollary 11. *Let $\mathbb{Z}$ be the ring of integers, $p_1, p_2, \ldots, p_k$, be prime integers, $r_1, r_2, \ldots, r_k$, be positive integers. Set $b_i = p_i^{r_i}$ for $i = 1, 2, \ldots, k$, $a = \prod b_i$, and $a_i = \prod_{i \neq j} b_j$. Then,*

$$\mathbb{Z}_a = e_1\mathbb{Z}_a + e_2\mathbb{Z}_a + \cdots + e_{k-1}\mathbb{Z}_a + e_k\mathbb{Z}_a,$$

where e_i is the unique nonzero idempotent in the ideal $a_i\mathbb{Z}_a \subsetneq \mathbb{Z}_a$, e_i is orthogonal to e_j whenever $i \neq j$, and the sum is a direct sum.

Proof. Denote by $\mathfrak{a}$, $\mathfrak{a}_i$, and $\mathfrak{b}_i$ the ideals generated by a, a_i, and b_i respectively. The idempotent e_i is an element of $\mathfrak{a}_i$. The orthogonality of e_i and e_j, $i \neq j$, follows from Corollary 8. By Corollary 7, the ideal $\mathfrak{a}_i/\mathfrak{a}$ is isomorphic to $\mathbb{Z}/\mathfrak{b}_i = \mathbb{Z}_{b_i}$ which is a local ring. The uniqueness of e_i follows from Lemma 2. The direct sum decomposition of $\mathbb{Z}_a$ follows from Corollary 9. □

It follows from Lemma 5, that given positive integers a, and b such that $\gcd(a, b) = 1$ then the ring

$$E_a = b\mathbb{Z}_a = \{0, b, 2b, \ldots, ab - b\}$$

is a ring under addition and multiplication modulo ab that is isomorphic to $\mathbb{Z}_a$. The ring E_a has multiplicative identity $(b^{\phi(a)} \bmod ab)$. This construction can be done for an infinite number of integers b but since it could happen that $(b^{\phi(a)} \neq b \bmod ab)$, b may not the multiplicative identity of E_a. However, we have the following proposition.

Proposition 12. *Let e be an integer, $e \geq 3$. Let b be a divisor of e, and $a > 1$ be a divisor of $e - 1$. Then, e is a nonzero idempotent in the ring $\mathbb{Z}_{ab}$ and is the identity of the ring E_a. Moreover, the map*

$$E_a \to \mathbb{Z}_a,\ x \bmod ab \mapsto x \bmod a,$$

is an isomorphism.

Proof. The proposition follows from Lemma 5 since $\gcd(a, b) = 1$. □

Next we observe that, if an integer $e \geq 3$ is an idempotent modulo n then $e(e - 1) = 0 \bmod n$. This implies that n must be a divisor of $e(e - 1)$. Since we want e to be a nonzero idempotent modulo a, n must be of the form $n = ab$ with a and b chosen as in the proposition. This proves the following corollary.

Corollary 13. *Let e be an integer, $e \geq 3$, and N_1 and N_2 be the number of divisors of e and $e - 1$ respectively. Then there are $N_1(N_2 - 1)$ integers of the form ab so that $(e \bmod ab)$ is the identity of the ring E_a.*

Example 14. *Consider the integer $e = 2016$. Since $2016 = 2^5 \cdot 3^2 \cdot 7$ and $2015 = 5 \cdot 13 \cdot 31$ we have $N_1 = 36$ and $N_2 = 8$. Therefore, there are $36 \cdot 7 = 252$ integers of the form ab (ab as in Proposition 12) such that $(2016 \bmod ab)$ is the identity of the ring*

$$E_a = \{0, e, 2e, \ldots, ae - e\}.$$

1. *Let $a = 5$ and $b = 2$. Then*

$$\begin{aligned} E_5 &= \{0, 2016, 4032, 6048, 8064\} \\ &= \{0, 6, 2, 8, 4\} \\ &= \{0, 2, 4, 6, 8\} \end{aligned}$$

   endowed with addition and multiplication modulo $10 = 2 \cdot 5$ is a ring with multiplicative identity $6 = 2016 \bmod 10$. E_5 is isomorphic to $\mathbb{Z}_5$.

2. *Let $a = 65$ and $b = 6$. Then*

$$\begin{aligned} E_{65} &= \{0, 2016, 4032, \ldots, 127008, 129024\} \\ &= \{0, 66, 132, \ldots, 258, 324\} \\ &= \{0, 6, 12, \ldots, 378, 384\} \end{aligned}$$

   endowed with addition and multiplication modulo $390 = 6 \cdot 65$ is a ring with multiplicative identity $66 = 2016 \bmod 390$. E_{65} is isomorphic to $\mathbb{Z}_{65}$.

3. *Let $a = 31$ and $b = 2016$. Then,*

$$E_{31} = \{0, 2016, 4032, \ldots, 58464, 60480\}$$

   endowed with addition and multiplication modulo $62496 = 31 \cdot 2016$ is a ring with multiplicative identity 2016. E_{31} isomorphic to the field $\mathbb{Z}_{31}$.

4. *Let $a = 7$ and $b = 288$. Since $288 - 1 = 287 = 7 \cdot 41$, then*

$$E_7 = \{0, 288, 576, 864, 1152, 1440, 1728\}$$

   endowed with addition and multiplication modulo $2016 = 7 \cdot 288$ is a ring with multiplicative identity 288.

4 Factor rings of the ring of Gaussian integers

In this section we will recall some properties of the Gaussian integers, define and compute an Euler function φ_G and give some examples of factor rings of the ring of Gaussian integers. First, recall that the Gaussian integers (denoted by $\mathbb{Z}[\mathbf{i}]$) is the sub-ring of the field of complex numbers given below

$$\mathbb{Z}[\mathbf{i}] = \{x + y\mathbf{i} \,|\, x \text{ and } y \text{ integers, } \mathbf{i}^2 = -1\}$$

endowed with addition and multiplication inherited from the field of complex number. The ring $\mathbb{Z}[\mathbf{i}]$ is an Euclidean domain with Euclidean function

$$\lambda : \mathbb{Z}[\mathbf{i}] \to \{0, 1, 2, 3, \ldots\}, \;\; \lambda(x + y\mathbf{i}) = x^2 + y^2.$$

Since $\mathbb{Z}[\mathbf{i}]$ is an Euclidean domain we have a division algorithm on it.

Theorem 15 (Division Algorithm for Gaussian Integers)**.** *Let $z_1 \neq 0$ and z_2 be Gaussian integers then there exist q and r Gaussian integers such that*

$$z_2 = qz_1 + r, \text{and } r = 0 \text{ or } \lambda(r) < \lambda(z_1).$$

Proof. Let $d = \lambda(z_1) \in \mathbb{Z}$. Write $z_2\overline{z}_1 = A + B\mathbf{i}$. By the division algorithm on the ring of integers, we can write A and B as $A = q_1 d + r_1$ and $B = q_2 d + r_2$ with $-\frac{d}{2} \leq r_1 \leq \frac{d}{2}$ and $-\frac{d}{2} \leq r_2 \leq \frac{d}{2}$. Therefore,

$$z_2\overline{z}_1 = A + B\mathbf{i} = (q_1 + q_2)d + (r_1 + r_2\mathbf{i}) = (q_1 + q_2\mathbf{i})z_1\overline{z}_1 + (r_1 + r_2\mathbf{i}).$$

Since $\overline{z}_1$ divides $z_2\overline{z}_1$ and $(q_1 + q_2\mathbf{i})z_1\overline{z}_1$, it follows that $\overline{z}_1$ divides $r_1 + r_2\mathbf{i}$. That is,

$$r = \frac{r_1 + r_2\mathbf{i}}{\overline{z}_1}$$

is a Gaussian integer. This shows that

$$z_2 = (q_1 + q_2\mathbf{i})z_1 + r.$$

Since, $-\frac{d}{2} \leq r_1 \leq \frac{d}{2}$ and $-\frac{d}{2} \leq r_2 \leq \frac{d}{2}$ either $r = 0$ or

$$\lambda(r) = \lambda\left(\frac{r_1 + r_2\mathbf{i}}{\overline{z}_1}\right) = \frac{\lambda(r_1 + r_2\mathbf{i})}{\lambda(\overline{z}_1)} = \frac{r_1^2 + r_2^2}{d} \leq \frac{(d/2)^2 + (d/2)^2}{d} = \frac{d^2/2}{d} = \frac{d}{2} < \lambda(z_1). \quad \square$$

The ring $\mathbb{Z}[\mathbf{i}]$, being an Euclidean domain, is a unique factorization domain. Therefore, if a is a Gaussian integer then a can be written uniquely (up to units) as the product of prime Gaussian elements. The following theorem characterizes the prime elements of $\mathbb{Z}[\mathbf{i}]$.

Theorem 16. *Let p be a prime in $\mathbb{Z}$. Then:*

1. *If $p = 2$, then $1 + \mathbf{i}$ is prime in $\mathbb{Z}[\mathbf{i}]$ and $2 = \mathbf{i}^3(1 + \mathbf{i})^2$.*
2. *If $p \equiv 3 \bmod 4$, then p remains prime in $\mathbb{Z}[\mathbf{i}]$.*
3. *If $p \equiv 1 \bmod 4$, then there exists a prime $\pi \in \mathbb{Z}[\mathbf{i}]$ such that $p = \pi\overline{\pi}$, and the primes π and $\overline{\pi}$ are nonassociate in $\mathbb{Z}[\mathbf{i}]$. Furthermore, every prime in $\mathbb{Z}[\mathbf{i}]$ is associate to one of the primes listed in (1)-(3) above. (Two primes are associate if they differ by a unit factor.)*

Proof. See [3] page 81. $\square$

Denote by $\langle a \rangle$ the ideal of $\mathbb{Z}[\mathbf{i}]$ generated by a and by $\mathbb{Z}[\mathbf{i}]_a$ the quotient ring $\mathbb{Z}[\mathbf{i}]/\langle a \rangle$. We have the following result.

Corollary 17. *Let $\mathbb{Z}[\mathbf{i}]$ be the ring of Gaussian integers, $\pi_1, \pi_2, \ldots, \pi_k$ be prime elements in $\mathbb{Z}[\mathbf{i}]$, $r_1, r_2, \ldots, r_k$ be positive integers, $a_l = \pi_l^{r_l}$ for $l = 1, 2, \ldots, k$, $a = \prod a_l$, and $b_l = \prod_{l \neq j} a_j$. Then*

$$\mathbb{Z}[\mathbf{i}]_a = e_1\mathbb{Z}[\mathbf{i}]_{b_1} + e_2\mathbb{Z}[\mathbf{i}]_{b_2} + \cdots + e_{k-1}\mathbb{Z}[\mathbf{i}]_{b_{k-1}} + e_k\mathbb{Z}[\mathbf{i}]_{b_k}$$

where e_l is the unique nonzero idempotent in the ideal $b_l\mathbb{Z}[\mathbf{i}]_a \subsetneq \mathbb{Z}[i]_a$, e_l is orthogonal to e_j whenever $l \neq j$, and the sum is a direct sum.

Proof. The proof is similar to the proof of Corollary 11, so we omit it. $\square$

We remark that Proposition 12 and Corollary 13 remain valid in the Gaussian integers setting. We also have the following theorem about factor rings of the ring $\mathbb{Z}[\mathbf{i}]$.

Theorem 18. *Let $z = a + b\mathbf{i}$ be a Gaussian integer then*

1. $\mathbb{Z}[\mathbf{i}]_{a+b\mathbf{i}} \cong \mathbb{Z}[\mathbf{i}]_{-a-b\mathbf{i}} \cong \mathbb{Z}[\mathbf{i}]_{b-a\mathbf{i}} \cong \mathbb{Z}[\mathbf{i}]_{-b+a\mathbf{i}}$
2. *If $a > 1$ and $b = 0$ then $\mathbb{Z}[\mathbf{i}]_{a+b\mathbf{i}} = \mathbb{Z}[\mathbf{i}]_a \cong \mathbb{Z}_a[\mathbf{i}]$*
3. *If $\gcd(a, b) = 1$ then $\mathbb{Z}[\mathbf{i}]_{a+b\mathbf{i}} = \mathbb{Z}_{a^2+b^2}$*
4. *If $n > 0$ is an integer then*
   (a) *If $n = 2m$, $\mathbb{Z}[\mathbf{i}]_{(1+\mathbf{i})^n} \cong \mathbb{Z}_{2^m}[\mathbf{i}]$.*
   (b) *If $n = 2m + 1$, $m \geq 1$ then $\mathbb{Z}[\mathbf{i}]_{(1+\mathbf{i})^n} \cong \mathbb{Z}[x]/\langle 2^m x, 2^{m+1}, x^2 + x + 2\rangle$. In this case, $\mathbb{Z}[\mathbf{i}]_{(1+\mathbf{i})^n}$ is not isomorphic to $\mathbb{Z}_c$, $\mathbb{Z}_c[\mathbf{i}]$, or to any direct product of rings of this type.*

Proof. See [4] Fact 1 and Theorems 1, 2, and 5. □

Example 19. *Consider the ring $\mathbb{Z}[\mathbf{i}]_{360}$. Let $z_1 = 1 + 2\mathbf{i}$. Since $360 = \mathbf{i} \cdot z_1 \cdot \overline{z}_1 \cdot 3^2 \cdot (1 + \mathbf{i})^6$ The sets*

$$\begin{array}{rcccl} Z_5 &=& \{x72(1+2\mathbf{i}) \mid x \in \mathbb{Z}_5\} &=& 72(1+2\mathbf{i})\mathbb{Z}[\mathbf{i}]_{360}, \\ \overline{Z}_5 &=& \{x72(1-2\mathbf{i}) \mid x \in \mathbb{Z}_5\} &=& 72(1-2\mathbf{i})\mathbb{Z}[\mathbf{i}]_{360}, \\ Z_8[\mathbf{i}] &=& \{45(x+y\mathbf{i}) \mid x, y \in \mathbb{Z}_8\} &=& 45\mathbb{Z}[\mathbf{i}]_{360}, \text{ and} \\ Z_9[\mathbf{i}] &=& \{40(x+y\mathbf{i}) \mid x, y \in \mathbb{Z}_9\} &=& 40\mathbb{Z}[\mathbf{i}]_{360} \end{array}$$

are principal ideals of $\mathbb{Z}[\mathbf{i}]_{360}$. These ideals are rings with unity under addition and multiplication modulo 360. The multiplicative identities of the ideals Z_5, $\overline{Z}_5$, Z_8 and Z_9 are $e_5 = 288 - 144\mathbf{i}$, $\overline{e}_5 = 288 + 144\mathbf{i}$, $e_8 = 225$, and $e_9 = 280$ respectively. The element 0 is the additive identity for them. The ring isomorphisms and their inverses are given below.

$$\begin{array}{rclrcl} \theta_{e_5} : Z_5 &\to& \mathbb{Z}[\mathbf{i}]_{1-2\mathbf{i}} & \theta_{e_5}(x72(1+2\mathbf{i}) \bmod 360) &=& x72(1+2\mathbf{i}) \bmod 1-2\mathbf{i} \\ \theta_{\overline{e}_5} : \overline{Z}_5 &\to& \mathbb{Z}[\mathbf{i}]_{1+2\mathbf{i}} & \theta_{\overline{e}_5}(x72(1-2\mathbf{i}) \bmod 360) &=& x72(1-2\mathbf{i}) \bmod 1+2\mathbf{i} \\ \theta_{225} : Z_8[\mathbf{i}] &\to& \mathbb{Z}_8[\mathbf{i}] & \theta_{225}(45(x+y\mathbf{i}) \bmod 360) &=& 45(x+y\mathbf{i}) \bmod 8 \\ \theta_{280} : Z_9[\mathbf{i}] &\to& \mathbb{Z}_9[\mathbf{i}] & \theta_{280}(40(x+y\mathbf{i}) \bmod 360) &=& 40(x+y\mathbf{i}) \bmod 9 \end{array}$$

$$\begin{array}{rclrcl} \theta_{e_5}^{-1} : \mathbb{Z}[\mathbf{i}]_{1-2\mathbf{i}} &\to& Z_5 & \theta_{e_5}^{-1}(x \bmod 1-2\mathbf{i}) &=& (288-144\mathbf{i})x \bmod 360 \\ \theta_{\overline{e}_5}^{-1} : \mathbb{Z}[\mathbf{i}]_{1+2\mathbf{i}} &\to& \overline{Z}_5 & \theta_{\overline{e}_5}^{-1}(x \bmod 1-2\mathbf{i}) &=& (288+144\mathbf{i})x \bmod 360 \\ \theta_{225}^{-1} : \mathbb{Z}_8[\mathbf{i}] &\to& Z_8[\mathbf{i}] & \theta_{225}^{-1}(x+y\mathbf{i}) &=& 225(x+y\mathbf{i}) \bmod 360 \\ \theta_{280}^{-1} : \mathbb{Z}_9[\mathbf{i}] &\to& Z_9[\mathbf{i}] & \theta_{280}^{-1}(x+y\mathbf{i}) &=& 280(x+y\mathbf{i}) \bmod 360 \end{array}$$

The elements, e_5, $\overline{e}_5$, e_8, and e_9 satisfy

$$e_5 \cdot \overline{e}_5 \equiv e_5 \cdot e_8 \equiv e_5 \cdot e_9 \equiv \overline{e}_5 \cdot e_8 \equiv \overline{e}_5 \cdot e_9 \equiv e_8 \cdot e_9 \equiv 0 \bmod 360$$

and

$$e_5 + \overline{e}_5 + e_8 + e_9 \equiv 1 \bmod 360$$

Therefore, for all $x \in \mathbb{Z}[\mathbf{i}]_{360}$, we have

$$xe_5 + x\overline{e}_5 + xe_8 + xe_9 \equiv x \bmod 360$$

and this representation is unique. That is,

$$\mathbb{Z}[\mathbf{i}]_{360} = e_5\mathbb{Z}[\mathbf{i}]_{360} \oplus \overline{e}_5\mathbb{Z}[\mathbf{i}]_{360} \oplus e_8\mathbb{Z}_{360} \oplus e_9\mathbb{Z}_{360}.$$

The other nonzero proper ideals of $\mathbb{Z}_{360}$ (besides Z_5, $\overline{Z}_5$, Z_8, Z_9) that are rings with addition and multiplication modulo 360 are

Ideal	*Identity*				
$Z_5 \oplus \overline{Z}_5$	$e_5 \oplus \overline{e}_5$	$\equiv$	$288 - 144\mathbf{i} + 288 + 144\mathbf{i}$	$\equiv$	$216 \bmod 360$
$Z_5 \oplus Z_8$	$e_5 \oplus e_8$	$\equiv$	$288 - 144\mathbf{i} + 225$	$\equiv$	$153 - 144\mathbf{i} \bmod 360$
$Z_5 \oplus Z_9$	$e_5 \oplus e_9$	$\equiv$	$288 - 144\mathbf{i} + 280$	$\equiv$	$218 - 144\mathbf{i} \bmod 360$
$\overline{Z}_5 \oplus Z_8$	$\overline{e}_5 \oplus e_8$	$\equiv$	$288 + 144\mathbf{i} + 225$	$\equiv$	$153 + 144\mathbf{i} \bmod 360$
$\overline{Z}_5 \oplus Z_9$	$\overline{e}_5 \oplus e_9$	$\equiv$	$288 + 144\mathbf{i} + 280$	$\equiv$	$218 + 144\mathbf{i} \bmod 360$
$Z_8 \oplus Z_9$	$e_8 \oplus e_9$	$\equiv$	$225 + 280$	$\equiv$	$145 \bmod 360$
$Z_5 \oplus \overline{Z}_5 \oplus Z_8$	$e_5 \oplus \overline{e}_5 \oplus e_8$	$\equiv$	$288 - 144\mathbf{i} + 288 + 144\mathbf{i} + 225$	$\equiv$	$81 \bmod 360$
$Z_5 \oplus \overline{Z}_5 \oplus Z_9$	$e_5 \oplus \overline{e}_5 \oplus e_9$	$\equiv$	$288 - 144\mathbf{i} + 288 + 144\mathbf{i} + 280$	$\equiv$	$136 \bmod 360$
$Z_5 \oplus Z_8 \oplus Z_9$	$e_5 \oplus e_8 \oplus e_9$	$\equiv$	$288 - 144\mathbf{i} + 225 + 280$	$\equiv$	$73 - 144\mathbf{i} \bmod 360$
$\overline{Z}_5 \oplus Z_8 \oplus Z_9$	$\overline{e}_5 \oplus e_8 \oplus e_9$	$\equiv$	$288 + 144\mathbf{i} + 225 + 280$	$\equiv$	$73 + 144\mathbf{i} \bmod 360$

Example 20. *Consider the integer $e = 2017$. Since we have the following prime power decomposition of 2017 and 2016 over the Gaussian integers*

$$2017 = (9 + 44\mathbf{i})(9 - 44\mathbf{i}) \text{ and } 2016 = 2^5 \cdot 3^2 \cdot 7 = \mathbf{i}^3(1 + \mathbf{i})^{10} \cdot 3^2 \cdot 7$$

we have $N_1 = 4$ and $N_2 = 66$. Therefore, there are $4 \cdot 66 = 264$ Gaussian integers of the form ab, where a is a divisor of 2017 and b is a divisor of 2016, so that $(e \bmod ab)$ is the identity of the ring $E_a = b\mathbb{Z}[\mathbf{i}]_a$ endowed with addition and multiplication modulo ab.

5 Factor rings of rings of polynomials

Let $\mathbb{F}$ be a field and $\mathbb{F}[x]$ be the ring of polynomials with coefficients in $\mathbb{F}$ and indeterminate x. The ring $\mathbb{F}[x]$ is an Euclidean domain with Euclidean function

$$\deg : \mathbb{F}[x] \to \mathbb{Z}^+ \cup \{0\}$$

where $\deg(f(x))$ is the degree of the polynomial $f(x)$.

Theorem 21 (Division Algorithm for Polynomial Rings)**.** *Let $d(x) \neq 0$ and $f(x)$ be elements of $\mathbb{F}[x]$ then there exists $q(x)$ and $r(x)$ elements of $\mathbb{F}[x]$ such that*

$$f(x) = q(x)d(x) + r(x), \text{and } r(x) = 0 \text{ or } \deg(r(x)) < \deg(d(x)).$$

Moreover, $q(x)$ and $r(x)$ are unique.

Proof. See [5] Theorem 16.2. □

Since $\mathbb{F}[x]$ is an Euclidean domain, it is a unique factorization domain. We have the following result.

Corollary 22. *Let $p_1(x), p_2(x), \dots, p_k(x)$, be irreducible polynomials in $\mathbb{F}[x]$, $r_1, r_2, \dots, r_k$, be positive integers. Set $b_i(x) = p_i(x)^{r_i}$ for $i = 1, 2, \dots, k$, $a(x) = \prod b_i(x)$, and $a_i(x) = \prod_{i \neq j} b_j(x)$. Let $\mathbb{F}[x]_{a(x)} := \mathbb{F}[x]/\langle a(x)\rangle$. Then,*

$$\mathbb{F}[x]_{a(x)} = e_1(x)\mathbb{F}[x]_{a(x)} + e_2(x)\mathbb{F}[x]_{a(x)} + \cdots + e_{k-1}(x)\mathbb{F}[x]_{a(x)} + e_k(x)\mathbb{F}[x]_{a(x)},$$

where $e_i(x)$ is the unique nonzero idempotent in the ideal $a_i(x)\mathbb{F}[x]_{a(x)} \subsetneq \mathbb{F}[x]_{a(x)}$, $e_i(x)$ is orthogonal to $e_j(x)$ whenever $i \neq j$, and the sum is a direct sum.

Proof. The proof is similar to the proof of Corollary 11. □

Example 23. *Let p be a prime and $q = p^r$. Let $\mathbb{F}_q$ be the finite field with q elements. Let n be a positive integer with $\gcd(p, n) = 1$ and $a(x) = x^n - 1$ be an element of $\mathbb{F}_q[x]$. The condition $\gcd(p, n) = 1$ implies that the factorization of $a(x)$ has not repeated factors, that is,*

$$a(x) = x^n - 1 = p_1(x) \cdot p_2(x) \cdots p_{k-1}(x) \cdot p_k(x)$$

where $p_i(x)$ is irreducible of degree d_i and $p_i(x) \neq p_j(x)$ if $i \neq j$. Corollary 22 implies that the factor ring $\mathbb{F}_q[x]_{a(x)} := \mathbb{F}_q[x]/\langle a(x)\rangle$ decomposes as the direct sum

$$\mathbb{F}_q[x]_{a(x)} = e_1(x)\mathbb{F}_q[x]_{a(x)} + e_2(x)\mathbb{F}_q[x]_{a(x)} + \cdots + e_{k-1}(x)\mathbb{F}_q[x]_{a(x)} + e_k(x)\mathbb{F}_q[x]_{a(x)}.$$

The ideal $e_j(x)\mathbb{F}_q[x]_{a(x)}$ is a field under addition and multiplication modulo $a(x)$, it is isomorphic to the field with q^{d_i} elements $\mathbb{F}_q[x]_{p_i(x)}$, and the idempotent element $e_j(x)$ is given by the formula $e_j(x) = a_j(x)^{q^{d_i}-1} \bmod a(x)$. The latter statement follows from the fact that the order of the group of units $U\left(\mathbb{F}_q[x]_{p_i(x)}\right)$ of the field $\mathbb{F}_q[x]_{p_i(x)}$ is $q^{d_i} - 1$. The idempotent elements $e_j(x)$ are known as primitive idempotent elements and they generate the minimal ideals of the factor ring $\mathbb{F}_q[x]_{a(x)}$.

This example is important because the ideals of the ring $\mathbb{F}_q[x]_{a(x)}$ correspond to $q-$ary cyclic error-correcting codes and the minimal idempotent elements correspond to the $q-$ary minimal cyclic codes. See Theorem 8.1 in [1] for a proof of this correspondence.

References

[1] J. Baylis, *Error-Correcting codes, a mathematical introduction*, Chapman and Hall Mathematics, 1998.

[2] R. I. Berger, *Hidden group structure*, Amer. Math. Monthly, **78**, (2005) 45-48.

[3] D. A. Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons Inc., 1989.

[4] G. Dresden and W. Dymàček, *Finding Factors Rings over the Gaussian Integers*, Amer. Math. Monthly, **112**, (2005) 602-611.

[5] J. A. Gallian, *Contemporary Abstract Algebra*, Houghton-Mifflin Company, 2002.

[6] K. R. McLean, *Groups in modular arithmetic*, The Mathematical Gazette, Vol. **62**, No. 420 (1978) 94-104.